

**SECRETARY OF STATE[721]**

**Adopted and Filed**

**Rule making related to elections technology security**

The Secretary of State hereby amends Chapter 29, “Elections Technology Security,” Iowa Administrative Code.

*Legal Authority for Rule Making*

This rule making is adopted under the authority provided in Iowa Code section 47.1.

*State or Federal Law Implemented*

This rule making implements, in whole or in part, Iowa Code section 47.1.

*Purpose and Summary*

While the Secretary of State’s office has seen tremendous voluntary adoption of services and security best practices, there is more work to do to continue to increase the security of Iowa’s elections. These amendments will bolster election security by requiring county commissioners of elections to uniformly adopt best practices.

*Public Comment and Changes to Rule Making*

Notice of Intended Action for this rule making was published in the Iowa Administrative Bulletin on March 11, 2020, as **ARC 4965C**. Comments were received from a county IT director. Most suggestions were accepted, and minor language changes based on those comments have been made.

*Adoption of Rule Making*

This rule making was adopted by the Secretary of State on April 15, 2020.

*Fiscal Impact*

This rule making has no fiscal impact to the State of Iowa.

*Jobs Impact*

After analysis and review of this rule making, no impact on jobs has been found.

*Waivers*

Any person who believes that the application of the discretionary provisions of this rule making would result in hardship or injustice to that person may petition the Secretary of State for a waiver of the discretionary provisions, if any, pursuant to 721—Chapter 10.

*Review by Administrative Rules Review Committee*

The Administrative Rules Review Committee, a bipartisan legislative committee which oversees rule making by executive branch agencies, may, on its own motion or on written request by any individual or group, review this rule making at its [regular monthly meeting](#) or at a special meeting. The Committee’s meetings are open to the public, and interested persons may be heard as provided in Iowa Code section 17A.8(6).

*Effective Date*

This rule making will become effective on June 10, 2020.

The following rule-making actions are adopted:

ITEM 1. Amend subrule 29.3(1) as follows:

**29.3(1)** A commissioner who identifies or suspects an actual or possible cybersecurity incident or breach shall ~~immediately~~ report the incident within 24 hours to the state commissioner. Upon receiving the report, the state commissioner shall alert the appropriate state or federal law enforcement agencies, including but not limited to the federal United States Department of Homeland Security, Security's Cybersecurity and Infrastructure Security Agency (CISA) and the OCIO, and the vendor responsible for maintaining the affected technology. The state commissioner may disseminate the information to other federal, state, and local agencies, or their designees, as the state commissioner deems necessary.

ITEM 2. Adopt the following new rule 721—29.4(47):

**721—29.4(47) Election security by the commissioners.**

**29.4(1)** At the start of each calendar year, the commissioner shall provide to the state commissioner the following information:

*a.* The full personnel roster, phone numbers, and email addresses of the commissioner's office that identify who from the office will participate in election administration in any form throughout the year. This does not include precinct election workers.

(1) The roster will identify the personnel that the commissioner considers critical to the successful execution of elections.

(2) The roster will further identify a technical point-of-contact (POC) for the state commissioner. If the commissioner wishes to serve as the POC, the commissioner will also designate an additional POC. The POC needs to be a government employee but does not necessarily need to be a person within the commissioner's office.

*b.* A list of other county employees who may be involved in the event of an incident in the county.

**29.4(2)** Every commissioner shall be a member of the Elections Infrastructure Information Sharing and Analysis Center. The state commissioner shall provide information on how to become a member upon request by a commissioner.

**29.4(3)** In every odd-numbered year, every commissioner shall request the following services from CISA. The state commissioner shall provide information on how to request services upon request by a commissioner. A commissioner, with prior written approval from the state commissioner, may choose to use a vendor other than CISA for substantively similar services. A failure of CISA to provide properly requested services to a commissioner does not constitute a technical violation for purposes of Iowa Code section 39A.6.

- a.* Cyber resilience review.
- b.* Risk and vulnerability assessment.
- c.* External dependencies management assessment.
- d.* Remote penetration testing.
- e.* Protective security assessment.

**29.4(4)** Every commissioner shall utilize the following services from OCIO. The state commissioner shall provide information on how to request services upon request by a commissioner. A commissioner, with prior written approval from the state commissioner, may choose to use a vendor other than OCIO for substantively similar services. A failure of OCIO to provide properly requested services to a commissioner does not constitute a technical violation for purposes of Iowa Code section 39A.6.

- a.* Intrusion detection system.
- b.* Endpoint malware detection.
- c.* Cybersecurity training, including phishing assessments.
- d.* Vulnerability management.

**29.4(5)** Every commissioner shall request a weekly vulnerability scanning by CISA.

**29.4(6)** A commissioner shall remediate all critical or high-risk vulnerabilities identified by any assessment.

**29.4(7)** The state commissioner may require every commissioner and commissioner's staff to participate in phishing assessments.

**29.4(8)** Commissioners may choose to participate in any other assessments or testing from vendors approved by the state commissioner. Commissioners shall notify the state commissioner when any assessments are scheduled.

**29.4(9)** The state commissioner may require a commissioner and commissioner's staff to participate in any assessment or training that the state commissioner arranges.

**29.4(10)** A commissioner shall use only county-issued email for the conduct of elections. This applies to all full-time and part-time staff of the commissioner as well as the commissioner. No other email addresses are permitted for full-time and part-time employees of the county who assist in any part of the administration or security of elections for the conduct of elections. However, this does not apply to precinct election officials who are not normally employed by the county on a regular basis in another capacity. This prohibition includes forwarding election business emails to a personal email address. This does not include out-of-band emails created and authorized as a part of a continuity of government plan or an incident response plan.

**29.4(11)** Any county information technology infrastructure that is used to access or conduct any part of elections in the state is subject to the following requirements:

*a.* Passwords to access the county network must be compliant with the standards enumerated by either the National Institute of Standards and Technology, the OCIO, or guidance issued by the state commissioner.

*b.* Session-lock timeout standards must be compliant with the standards enumerated by either the National Institute of Standards and Technology or guidance issued by the state commissioner.

*c.* A current inventory of IT assets assigned to the commissioner's office shall be kept.

*d.* Daily, weekly and monthly data backups within the commissioner's office will be maintained and physically or logically separated from production data.

**29.4(12)** The website of a commissioner shall have a top-level domain of ".gov" and shall utilize secure socket layer or transport layer security certificates for all publicly facing websites. A commissioner's agreement with OCIO to use a subdomain of ".iowa.gov" is sufficient to satisfy this requirement. A commissioner's site that redirects traffic from a different top-level domain to a ".gov" domain is sufficient to satisfy this requirement.

**29.4(13)** If the state commissioner is satisfied that a county has an adequate alternative to any requirement in this rule, the state commissioner may waive that requirement. It is the sole discretion of the state commissioner whether a county qualifies for a waiver.

**29.4(14)** Except where otherwise exempted, failure by a commissioner to follow these rules constitutes a technical violation pursuant to Iowa Code section 39A.6.

ITEM 3. Adopt the following **new** rule 721—29.5(47):

**721—29.5(47) Emergency or incident response plans.**

**29.5(1)** Every commissioner shall have an election security incident response plan. A commissioner whose election-specific plan is part of a larger county-level emergency response plan, continuity of government plan, or incident response plan satisfies this requirement.

**29.5(2)** Every commissioner shall review the plan at least annually and make updates as necessary.

**29.5(3)** A commissioner shall provide the plan to the state commissioner at the state commissioner's request.

**29.5(4)** Information shared under this rule shall retain protection as a nonpublic, confidential record pursuant to Iowa Code section 47.1(6).

ITEM 4. Adopt the following **new** rule 721—29.6(47):

**721—29.6(47) Social media accounts.**

**29.6(1)** A commissioner using a social media account for official elections-related communication shall request “verified” or similar recognition. The state commissioner shall provide information on the subject upon request by a commissioner.

**29.6(2)** A commissioner using a social media account shall protect the account using multifactor authentication.

**29.6(3)** The state commissioner may require that commissioners use additional security measures for social media accounts, based on emerging best practices.

[Filed 4/16/20, effective 6/10/20]

[Published 5/6/20]

EDITOR’S NOTE: For replacement pages for IAC, see IAC Supplement 5/6/20.